REMARKS

The application was filed on 19 April 2001 with sixteen claims. The Examiner examined the application and on 21 October 2004 issued a first Action. In the Examiner's Action, the Examiner rejected claims 1-7 and 10-16 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,405, 364 B1 entitled BUILDING TECHNIQUES IN A DEVELOPMENT ARCHITECTURE FRAMEWORK to Bowman-Amuah (Bowman-Amuah '364). The Examiner also rejected claims 8-9 under 35 U.S.C. §103(a) as being unpatentable over Bowman-Amuah '364 in view of U.S. Patent No. 5,519,778 entitled METHOD FOR ENABLING USERS OF A CRYPTOSYSTEM TO GENERATE AND USE A PRIVATE PAIR KEY FOR ENCIPHERING COMMUNICATIONS BETWEEN THE USERS to Leighton et al. (Leighton '778).

In response, Applicants amended the specification and claims. The Examiner responded with a final rejection of claims 1-7 and 10-16 under 35 U.S.C. §103(a) as being unpatentable over Bowman-Amuah '364 in view of U.S. Patent No. 4,672,572 entitled PROTECTOR SYSTEM FOR COMPUTER ACCESS AND USE to Alsberg (Alsberg '572). The Examiner finally rejected claims 8 and 9 under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572, and Leighton '778. In response, Applicants have amended the claims to put them in condition for allowance and/or better condition for appeal. Applicants respectfully request the Examiner to enter the amendments and pass the application to issuance.

In amending claims 1 and 7, Applicants have not added new matter. Support in the original filed specification for the invention using a baseline to determine security properties and functions is given on page 8, lines 12-18, which states, "[t]he present invention uses a set of baseline requirements for security and a security design method to achieve a simple, yet repeatable method and system for designing a solution with integrated security. The present invention also includes a variety of baseline tools and procedures. However, since the tools of the present invention are not mutually exclusive, they allow for the mixing and matching. Under some circumstances, some of the tools may be used without the corresponding use of other tools." Support for the subsystems of the second system being the baseline tools is given on page 17, line 23

through page 18, line 3 which states, "the processes of the credential, access control and information control subsystems are spread through the three domains (but, for simplicity, the present example does not include any audit or integrity subsystems although these could be added, if desired, to the environment, based on the foregoing explanation of these subsystems." In amending claims 5 and 11, Applicants have not added new matter. Support in the original specification for "assurance" requirement is given on page 11, lines 18-19 which states, "[t]he Common Criteria are also used at block 112 to develop assurance requirements for the solution." In amending claims 7, 8 and 9, Applicants have not added new matter. Support in the originally filed specification is given on page in current claim 8 and 9 which evaluates and ranks the threats to the security properties of the overall solution; the specification on page 11, lines 12-13 states that "the security properties of the overall solution are determined in terms of the security subsystems." Claims 1-16 are pending.

The Rejection Under 35 U.S.C. §103(a) over Bowman-Amuah '364 and Alsberg '572

The Examiner rejected claims 1-7 and 10-16 under 35 U.S.C. §103(a) as being unpatentable over Bowman-Amuah '364. The Examiner asserts that Bowman-Amuah '364 discloses a system and method for building systems in a development architecture framework wherein security is integrated into the solution. The Examiner admits that Bowman-Amuah '364 does not disclose a security subsystem that includes an audit subsystem, an integrity subsystem, and an information flow control subsystem. The Examiner then relies on Alsberg '572 to providing a protector device for enhancing security including the audit subsystem, integrity subsystem, and information flow control subsystem. Thus, the Examiner reasons that one of skill in the art would be inclined to combine Bowman-Amuah '364 with Alsberg '572 because auditing potentially sensitive material, integrity subsystems, and controlling the information flow would increase the security of the system.

In response, Applicants have amended independent claims 1 and 7, dependent claims 5, 8, 9 and 11. The amendments have narrowed the claims to particularly point out and distinctly claim that the second system comprises a plurality of baseline tools and that the subsystems of the second system are interconnected and interdependent.

Bowman-Amuah '364 teaches an integrated development framework for the creation of software that has security management. The most detail that Bowman-Amuah '364 provides for security management is presented at column 49, line 65 through column 51, line 13. The security management system of Bowman-Amuah '364 deals mainly with preventing unauthorized access to the system, e.g., *intrusion detection, network assessment, platform security to minimize the opportunities for intruders ..., web-based access control, fraud services, mobile code security, e-mail, encryption, public key infrastructure, authentication system, and firewall.* Bowman-Amuah '364 briefly mentions the need for security audits for the development architecture framework at column 18, lines 60-63, but merely states that audits can be done by an external body specializing in security in the form of interviews, architecture and code reviews, and automated tool assessment.

Alsberg '572 describes a protector device, also called security server, to be attached to a network of computers and terminals. The security server that is "independent from the host computer and terminals but connected to the computers and terminals ...." Alsberg '572 at column 4, lines 1-3. The security server does include such a command-filter module which generates an audit-capture command only when potentially sensitive information is transmitted, Alsberg '572 at column 6, lines 36-39, suggested by the Examiner to be akin to the claimed audit subsystem. The security server also has an administrator monitor that has a data base editor, an audit-trail analysis module, a status module, and a system-control module, Alsberg '572 at column 7, lines 4-6, allegedly the same as the claimed integrity subsystem. The security server has a user authentication module that monitors all input from and output to the user terminal (Alsberg '572 at column 8, lines 15-17); the Examiner suggests that the user authentication module is the claimed information flow control subsystem.

Respectfully, Applicants traverse the rejection based on 35 U.S.C. §103(a) because neither Bowman-Amuah '364 nor Alsberg '572 suggest that their combination would yield an integrated design process and reference model. Bowman-Amuah '364 admits that the audit function would be independent from the security management system. Alsberg '572 also states that the security server is independent from the host

computer and terminals. Therefore, because the first reference talks about an independent audit security function and because the second reference states that the security functions, i.e., audit, information flow control, and administrative control are independent from the system; the combination of an independent function with an independent security server simply cannot support a prima facie case of obviousness of an integrated security design method and model. Despite the Examiner's creativity, the suggested combination of Alsberg '572 with Bowman-Amuah '364 still does not yield the claimed invention because neither reference teaches the interdependence and interconnectedness among the subsystems, as claimed. First, Alsberg '572 teaches away from an interconnected and interdependent functions within the design of the system because it simply attaches a security server with its own functions onto a computer and terminals and specifically states that the security functions are independent of the host and terminal functions. Bowman'Amuah '364 merely provides a laundry list of security functions and components but doesn't state how they are to be integrated during the design process. Inventors' claimed method and system for designing security into a system having interconnected and interdependent audit, information control, and integrity subsystems as a baseline model is not rendered obvious by merely adding a security server to a pre-existing network; or by a list of security functions that could be accomplished by an independent security server.

In view of the amendments above, Applicants respectfully request the Examiner to withdraw the rejection of claims 1–7 and 10-16 under 35 U.S.C. §103(a) over Bowman-Amuah '364 in view of Alsberg '572 because tacking on an independent security server to a host computer system after it has been designed does not teach or suggest the integration of auditing, integrity, and information flow control as a baseline reference to determine the overall security properties of a solution.

The Rejection of claims 8-9 Under 35 U.S.C. §103(a) over Bowman-Amuah '364, Alsberg '572 in view of Leighton '778

The Examiner rejected claims 8-9 under 35 U.S.C. §103(a) under a combination of Bowman-Amuah '364 and Alsberg '572 in view of Leighton '778. The Examiner applies Bowman-Amuah '364 and Alsberg '572 as above and then applies Leighton '778 as a reference to rank the security levels and threats to the system. Applicants reiterate that Bowman-Amuah '364 and Alsberg '572 alleged combination of connecting an external security server to a laundry list of security components does not create the claimed integrated design process and baseline model for interconnecting interdependent security properties, such as audit, integrity and/or the information flow control of an integrated system.

Leighton '778 applies a ranking system to users of a cryptosystem wherein communications are ciphered between ranked users of the system, i.e., one user may have a higher security clearance/level than another user. Leighton '778 ranks only those users for secret-key exchange wherein first, users can directly talk to one another and second the conversation between two users always takes place at the highest common level of security, see column 6, lines 44-47. Leighton '778 does not suggest applying a ranking of security threats to the subsystems of a software development system or to an overall solution, as claimed by Applicants. Threats to management of audits, integrity, and information flow control are not mentioned by Leighton '778. Thus, with the Examiner's observation that Bowman-Amuah '364 does not rank security threats combined with the fact that Leighton '778 ranks only the security level of users on a cryptographic system, Applicants respectfully request the Examiner to reconsider the rejection of claims 8 and 9 under 35 U.S.C. §103(a) and allow the claims.

Conclusion

Applicants maintain that the security management proffered by Bowman-Amuah '364 does not teach nor suggest, nor can be easily modified to integrate the three process subsystems claimed in independent claims 1 and 7 of Applicants' invention. The teachings, moreover, of Alsberg '572 of adding an external security

server to a preexisting system, such as Bowman-Amuah '364, still does manifest the claimed design process having at least three interdependent and interconnected subsystems that act as a baseline reference into which security can be designed. The combination of Bowman-Amuah '364 and Alsberg '572 with Leighton '778, moreover, does not teach the three subsystems integrated into security wherein the risks to the auditing, the risks to the integrity, and the risks to the information flow control subsystems are ranked.

Attorney for Applicants thank the Examiner for her careful review of the specification, the figures, and the claims. Applicants have thus amended the claims to place the claims in condition for allowance and/or better condition for appeal. Applicants request the Examiner to enter the amendments and allow all claims. The Examiner is further invited to telephone the Attorney listed below if she thinks it would expedite the prosecution and the issuance of the patent.

Respectfully submitted,
A. M. Gilbert et al.

Date: 13 September 2005

By _____
Karuna Ojanen
Registration No. 32,484
(507) 282-0049 voice
(507) 281-5722 fax

OLO - Ojanen Law Offices
1530 Greenview Drive, SW
Suite 212
Rochester, MN 55902-1080